Non-Traditional Uses of Forensics in Security Analysis

Steven Kaplan, CISSP, CISA
Accuvant
skaplan@accuvant.com
Sandra Bittner, CISSP
Arizona Public Service
Palo Verde Nuclear Generating Station

The Challenge:

- Commercial generation facilities must identify malware and exposed vulnerabilities on production systems without introducing configuration changes to the systems examined.
- Commercial production must not sustain unplanned interruptions

The Forensic Advantage

- Traditionally forensic tools are limited to evidence recovery and support of legal action or police investigations.
- Tools developed for forensic science can do more and solve more problems efficiently.

The Answer

- Use forensic tools to create/capture an exact duplicate of the target systems without leaving any artifacts behind
- Use captured image to analyze the forensics copy for security issues (malware, exposed vulnerabilities) without impacting production systems.

The Benefits of a New Approach

- The new approach saves time, effort and money, and, will ***reduce*** *the attack surface area*.
- Examples of savings:
  - Previous required many laptops with a complement of scanning tools ($$$$), new requires only one system.
  - Manual isolation between systems and security levels are achieved.
  - Less opportunity for human performance issues and errors in the field.

Overview of New Approach

- Use a portable forensics tool to get a forensics copy of a Protected System computer.
- Import the evidence file into forensics SW
- Reconstruct the original image with forensic Physical Disk Emulator
- Scan the reconstructed image with a resident virus scanner, i.e. McAfee.
- Use a virtual forensics tool to take the emulated disk from EnCase and boot the target as a virtual machine.
- Now scan the virtual image just as if you were connected to the actual production system.

Cautions:

- Knowledge of Administrative system password is still required
- Alternatively, reuse tool VFC2 to bypass all the passwords.

Favorite Security Tools still work

- Nessus:
  - Now create a Nessus scan policy including an Administrator credential so you can execute a “Credential Scan”.
  - You may use all default plugins for “Internal Scan Policy”
  - Export scan when done.
- Nmap, WinAudit:
  - Perform traditionally and accurately

Additional Benefits

- The approach outlined not only protects the actual system from any deleterious impact from potentially abusive scanning tools, it..
  - Allows malware checking for systems that would normally be too old to be supported by A/V vendors
  - Allows cyber security to test other high risk scenarios without threatening production or safety.
  - Achieves increased flexibility:
    - Can gauge impact of changes, patches, pen testing on virtual image, before anything ever implemented on target system.

What investment is required?

- What is required?
  - About $5000 in specialized software
  - About $2000 for a high performance HW platform
  - Scanning tools of your choice, about $1500.
- Comparison: new (forensics) approach is equivalent to original method of actual scanning of target – without the risks.

Required Tools

- "**EnCase® Portable** - is a powerful solution, delivered on a USB device, that allows forensic professionals and non-experts to quickly and easily triage and collect vital data in a forensically sound and court-proven manner."

No Files Left are Behind by Encase Portable

EnCase Portable has “Three Operating Modes:

- Execute EnCase Portable on an already running computer (Live Mode)
- Boot a computer with EnCase Portable (Boot Mode)
- ***In either mode, no EnCase files are installed on the suspect’s computer” – EnCase_Portable _Brochure***

Tool Lineup:

Tool	Description
EnCase® Forensic	the industry-standard computer investigation solution, is for forensic practitioners who need to conduct efficient, forensically sound data collection and investigations using a repeatable and defensible process.
VMware Workstation	supports bridging existing host network adapters and share physical disk drives and USB devices with a virtual machine. In addition, it can simulate disk drives. It can mount an existing ISO image file into a virtual optical disc drive so that the virtual machine sees it as real one.
VFC2	is one of the significant breakthrough's in forensic computing in the last ten years. VFC enables investigators to: rapidly boot a forensic image of a suspects computer; or boot a physical write blocked hard drive. *VFC2 can side step all passwords on forensic images*

Security Tools

Tool	Description
Nessus	a proprietary comprehensive vulnerability scanner which is developed by Tenable Network Security.
Nmap	provides a variety of features for probing computer networks such as host discovery, service and operating system detection, and other more in depth system information.
WinAudit	PC audit and inventory of software, licenses, security configuration, hardware, network settings.

VM Forensic Tools

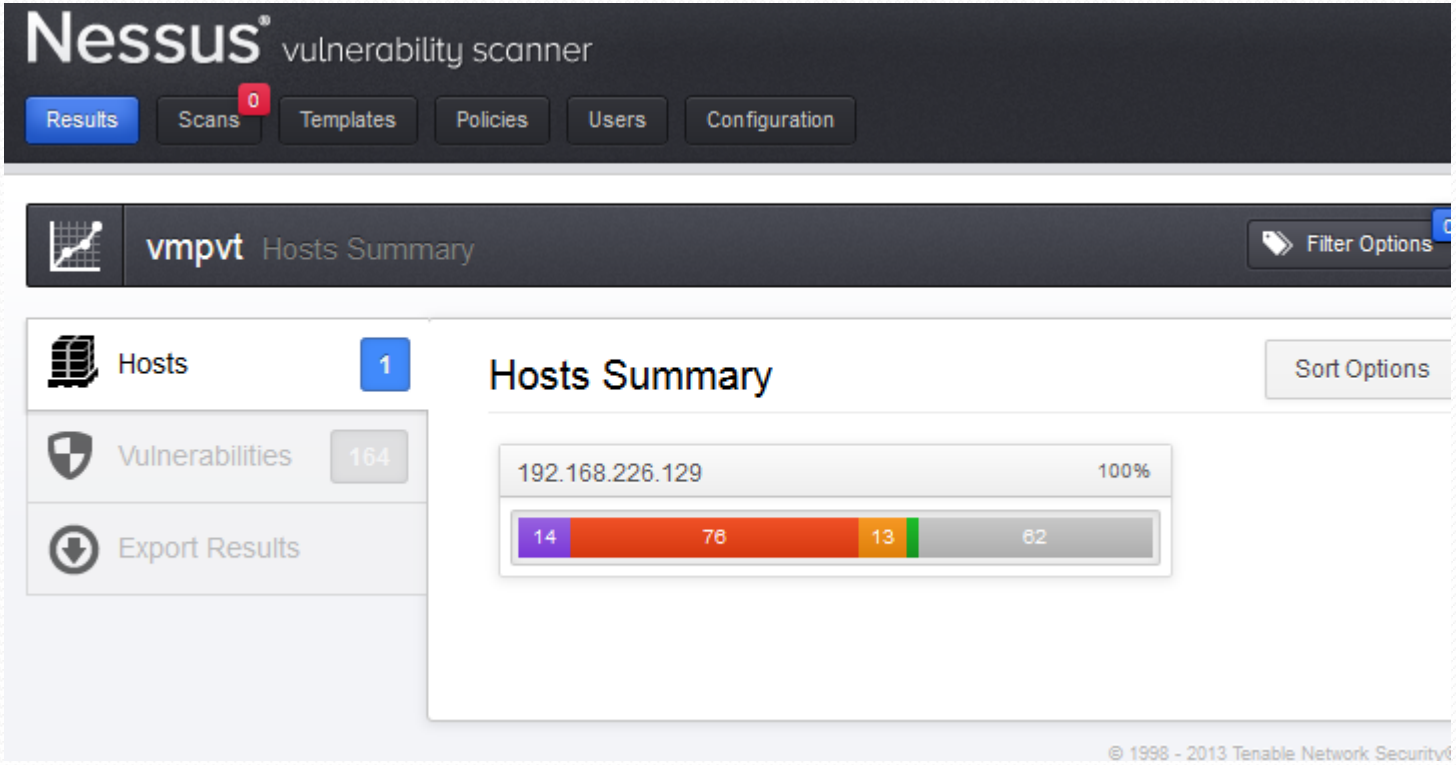
- At this writing, we tested two tools to boot (create VM images) from EnCase forensic images:
  - LiveView (which is free) and
  - VFC2 (which sells for $1000)
    - VFC2 works more reliably and has more features than LiveView.

VM Config

- A successful vmdk config generation by VFC2 will result in the creation of those files necessary to enable the subject mounted disk image to be booted in a VM
- This can be achieved by using the ‘Launch’ button located at the lower right of the main dialog screen.

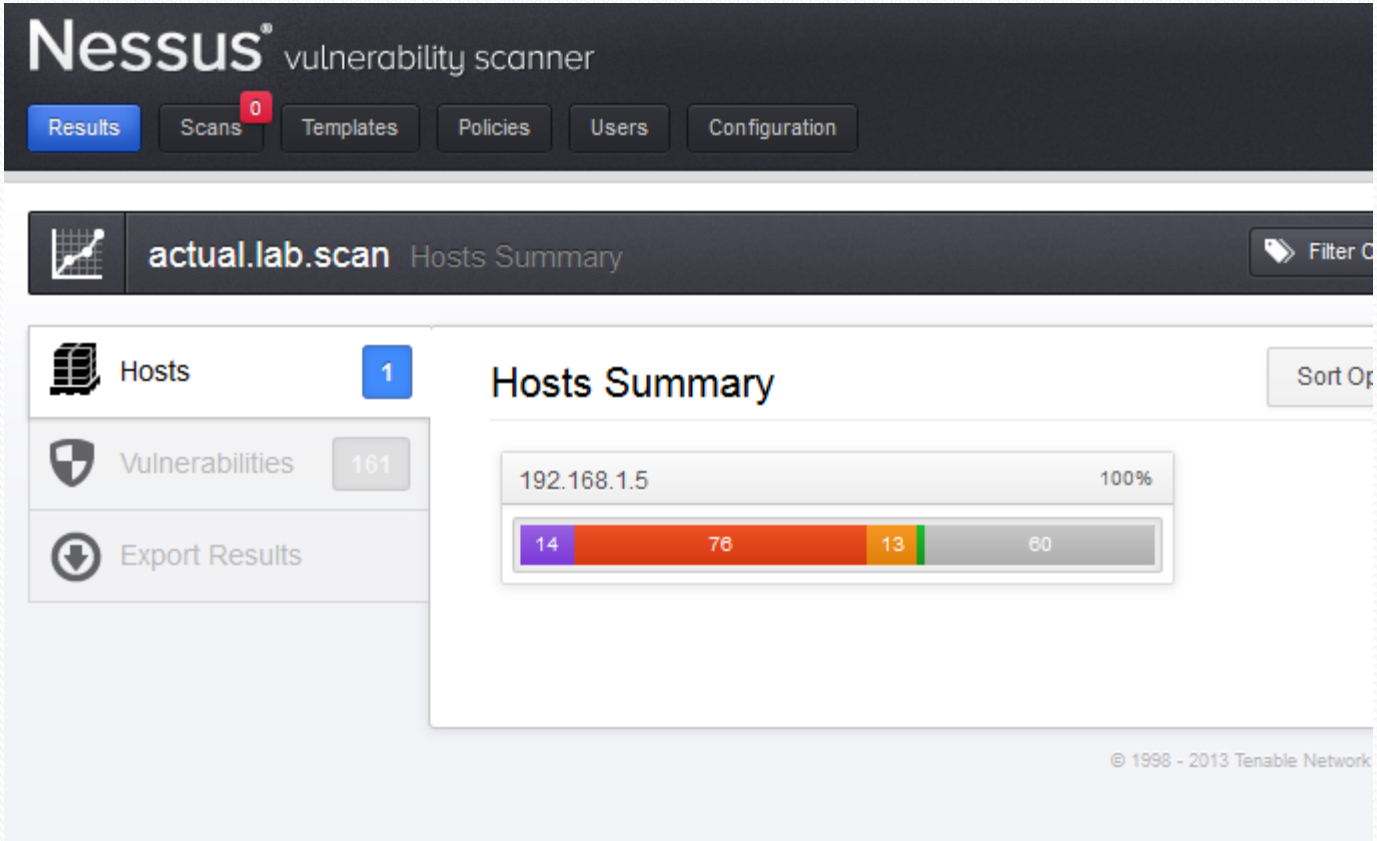
Comparison of Results

A scan of virtual machine



Comparison of Results

- Scan of same machine, done remotely



Conclusion

- The scans are equivalent, with the exception of some low level informational findings because one system is virtual machine
- Otherwise the findings are identical, and
- The VM process is a good, if not better approach.